(12) UK Patent Application (19) GB (11) 2 293 476 (13) A

(43) Date of A Publication 27.03.1996

(21) Application No 9519627.5

(22) Date of Filing 26.09.1995

(30) Priority Data
(31) 06229657 (32) 26.09.1994 (33) JP

(51) INT CL[6]
G06K 7/01

(52) UK CL (Edition O )
G4M MAW MB3

(56) Documents Cited
US 4322613 A

(58) Field of Search
UK CL (Edition N ) G4M MAW
INT CL[6] G06K 7/00 7/01 7/08 17/00
Online:WPI

(71) Applicant(s)
Kabushiki Kaisha Sankyo Seiki Seisakusho

(Incorporated in Japan)

No 5329 Shimosuwa-machi, Suwa-gun, Nagano, Japan

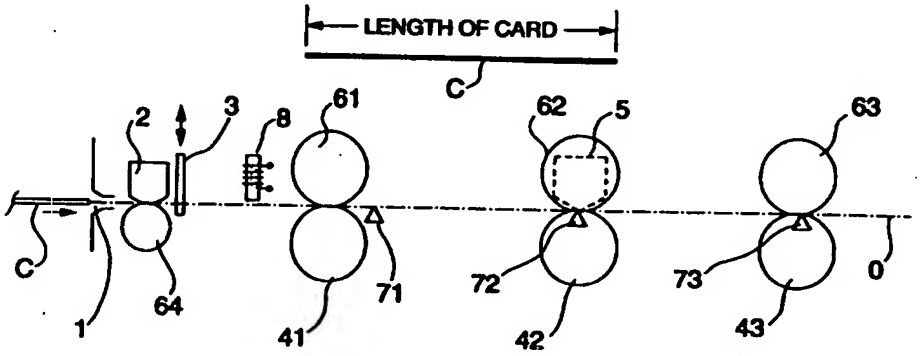
(72) Inventor(s)
Junji Ohwa
Kenji Hirasawa

(74) Agent and/or Address for Service
Brookes & Martin
High Holborn House, 52-54 High Holborn, LONDON, WC1V 6SE, United Kingdom

(54) Magnetic card reader

(57) Stored information is destroyed when a card C is intentionally pulled out of a magnetic card reader of the card running type. An abnormal stoppage of a running magnetic card is detected, a movement of the card after the stoppage is detected, and a magnetic information destruction device 8 is activated in response to the movement detection. When adjacent card sensors 71, 72, 73 do not detect a card for a time period which is longer than a preset time period, it is judged that the card is stopped.

FIG. 1




GB 2 293 476 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

FIG. 1

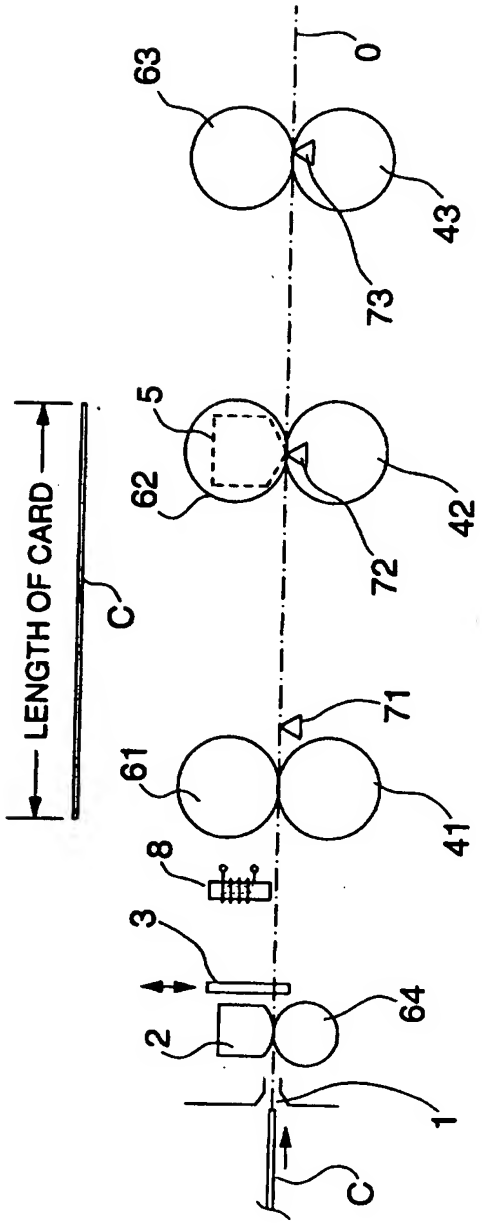


FIG. 2

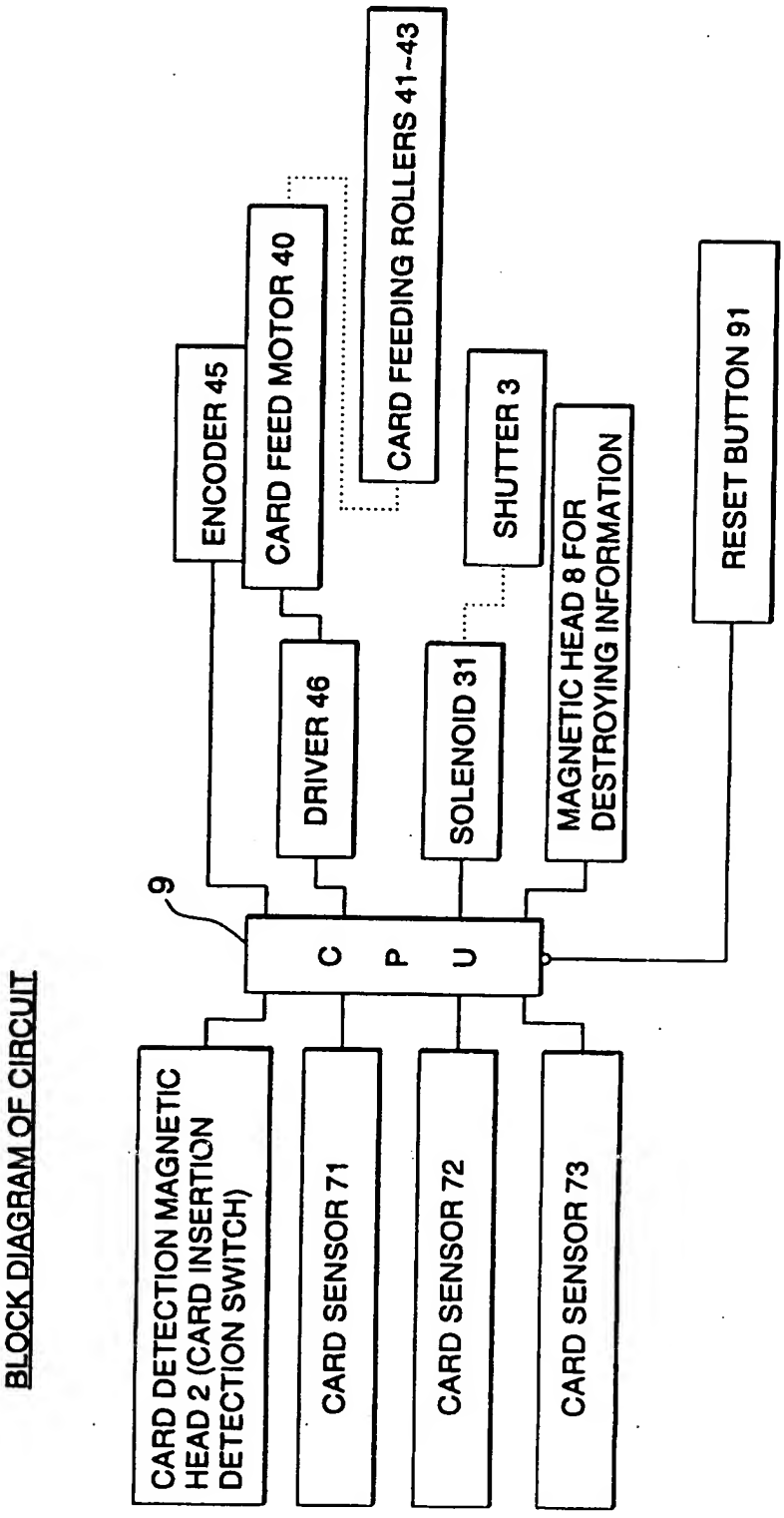

BLOCK DIAGRAM OF CIRCUIT
9
C
P
U
CARD DETECTION MAGNETIC HEAD 2 (CARD INSERTION DETECTION SWITCH)
CARD SENSOR 71
CARD SENSOR 72
CARD SENSOR 73
DRIVER 46
SOLENOID 31
MAGNETIC HEAD 8 FOR DESTROYING INFORMATION
RESET BUTTON 91
ENCODER 45
CARD FEED MOTOR 40
CARD FEEDING ROLLERS 41~43
SHUTTER 3

*FIG. 3* [FLOWCHART OF DETECTING STOPPAGE OF CARD]

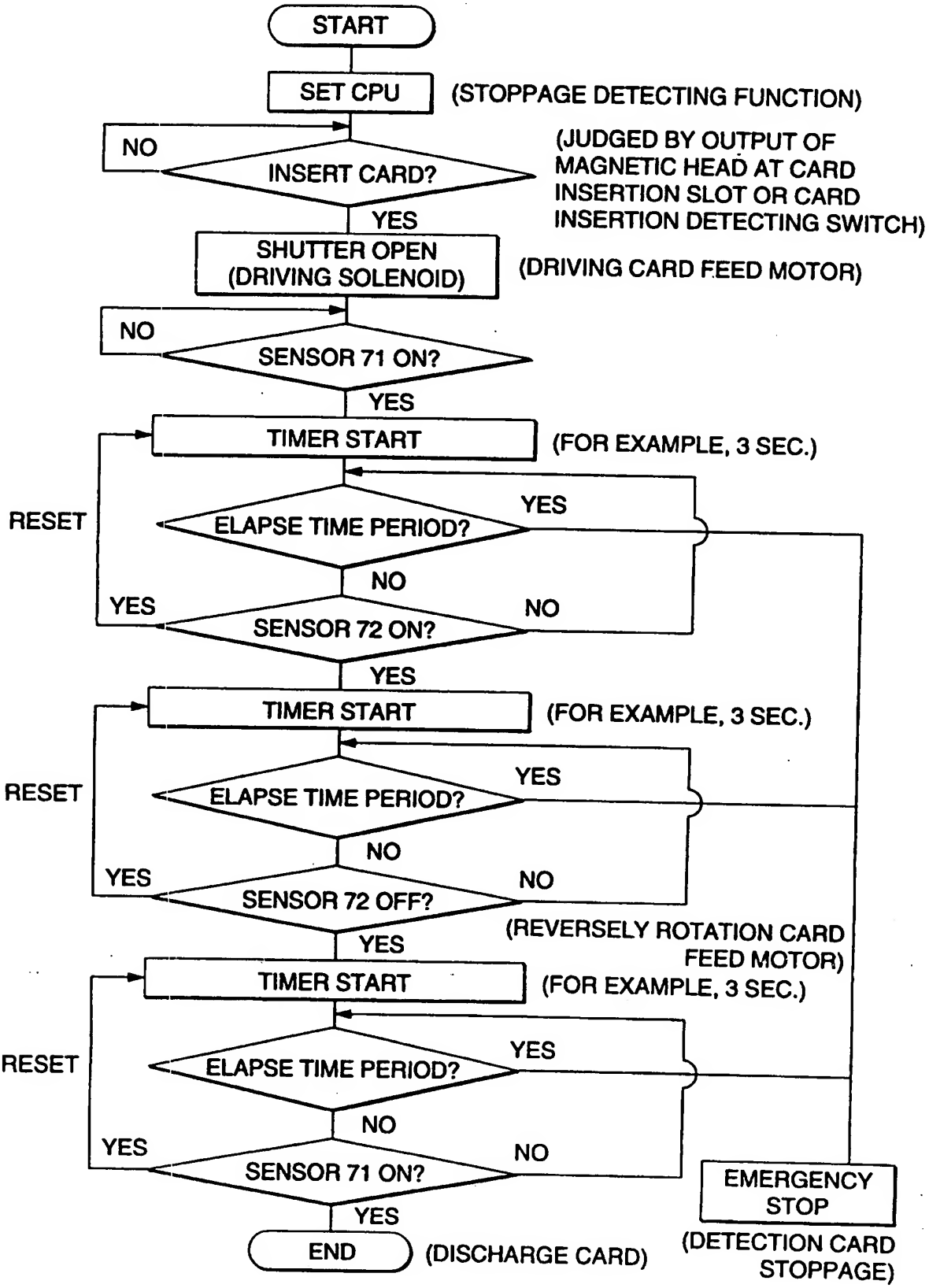
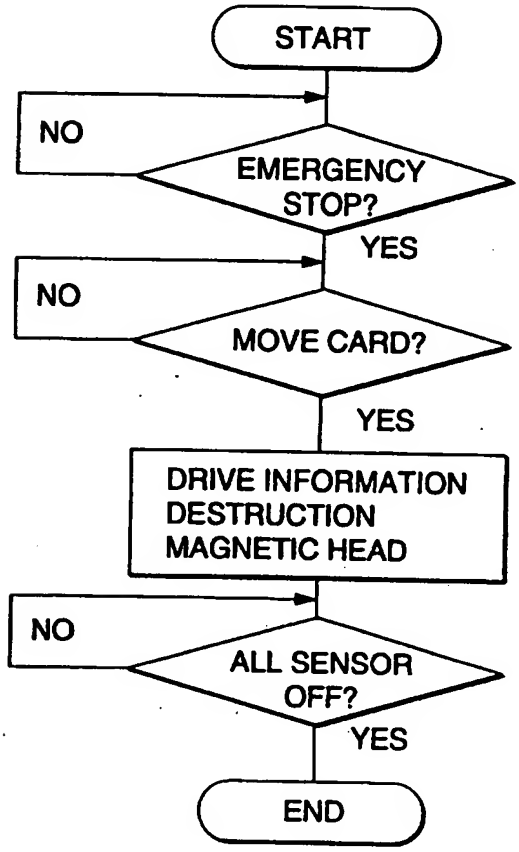


FIG. 4

[FLOWCHART OF OPERATION OF DESTROYING STORED INFORMATION OF CARD]



# METHOD OF PREVENTING A MAGNETIC CARD FROM BEING FRAUDULENTLY USED, AND A CARD READER

## BACKGROUND OF THE INVENTION

### Field of The Invention

This invention relates to a technique of preventing a magnetic card frequently used as a credit card or the like, from being fraudulently used, and more particularly to an improvement of a technique of preventing a magnetic card from being used by steal.

### Background

Magnetic cards such as credit cards which are based on accounts of banks, etc. are widely used as cashless device. Usually, a single person uses a number of magnetic cards.

Such a magnetic card allows dealings for cash to be automatically performed. Therefore, there is a problem in that, when a magnetic card is used by steal, extensive damage may be caused.

To comply with this, a magnetic card is provided with security device such as an addition of a password. In practice, when the password of a magnetic card is once known, however, the magnetic card is easily used fraudulently.

In place of cash, prepaid cards such as phonecards are widely used. When such a prepaid card is once stolen, it is impossible to prevent the prepaid card from being used by

steal. Furthermore, oblique dealings are often practiced in which the amount of a card is kept full by pulling out the card before settlement.

In order to prevent such fraud from occurring, a technique is proposed in Japanese Utility Model publication No. Hei. 4-28374 entitled "CARD READER". The proposed technique can be applied to a card reader having a special configuration in which a magnetic card is placed on a card tray and then introduced into the card reader, the tray is stopped at a normal position, and a magnetic head is caused to run on the card to read and write information such as an amount. According to the technique, a destruction unit which, when the tray is at the normal position, butts against a magnetic storage portion of the card is advanced into the vicinity of the card insertion slot. When the card is intentionally pulled out before the completion of the information reading and writing process, the destruction unit destroys the information of the magnetic storage portion so that the card is disabled to be again used.

In a card reader which is commonly used, however, a magnetic card is caused to run so as to be made slidingly contact with a magnetic head located at a normal position, thereby reading and writing information.

In card readers of this type, fraud has frequently been practiced in the following manner. A card reader is previously modified so that a card is intentionally stopped in the reader.

when a normal user inserts a magnetic card into the card reader, the card is stopped in the card reader and not returned to the user. After making sure that the user gives up the recovery of the card and leaves the card reader, the stopped card is pulled out. Such fraud can be repeatedly conducted.

## SUMMARY OF THE INVENTION

The problem to be solved by the invention is the above-described fraudulent use. Fundamentally, in the same manner as the above conventional example, the problem can be solved by, when a card is fraudulently pulled out, destroying information stored in the card. However, the above conventional example cannot attain a fraudulent use prevention method which can be applied to a magnetic card reader of the card running type, particularly to a magnetic card reader having a normal configuration.

The invention has an objection of providing a technique of destroying stored information which is to be conducted when a card is intentionally pulled out in a magnetic card reader of the card running type.

According to the invention there is provided a method of preventing a cared with stored information data from being fraudulently used in a card reader of the card running type, said method comprising the step of destroying at least a part of the information data stored in the card by an information destruction device when the card is fraudulently pulled out from the card reader.

Furthermore, there is provided a card reader device of the card running type for preventing a card with stored information data from being fraudulently used, said card reader comprising:

a stoppage detecting device for detecting an abnormal stoppage of the card,

a movement detecting device for detecting a movement of the card after the abnormal stoppage: and

an information destruction device for destroying at least a part of the information data, said information destruction device being activated in response to the movement of the card detected by said movement detecting device.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram showing the fundamental configuration of the card reader of the invention and the length of a card;

Fig. 2 is a block diagram of a circuit for controlling

the operation of Fig. 1;

Fig. 3 is a flowchart of a process of detecting the stoppage of the magnetic card; and

Fig. 4 is a flowchart of a process of destroying stored information.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Hereinafter, embodiments of the invention will now be described in detail with reference to Figs. 1 to 4.

Fig. 1 is a diagram showing the fundamental configuration of a card reader and the length of a card. In a card running path 0 which is disposed inside with respect to a card insertion slot 1, the following components are disposed: a card detection magnetic head 2 at a position corresponding to a magnetic stripe of an inserted magnetic card C; a magnetic head 8 for destroying magnetic information; a shutter 3 which can blocks the card insertion and, in the case of a normal card, is driven by driving device such as a solenoid 31 to open the card running path 0; card feeding rollers 41 to 43 which are arranged at intervals shorter than the length of the card and driven by a card feed motor 40; a pat roller 64 which opposes the magnetic head 2, driven rollers 61 to 63 which oppose the card feeding rollers 41 to 43, respectively; a magnetic head 5 which is adjacent to the side of the driven roller 63 and reads and writes magnetic information; and card sensors 71 to 73 which are arranged in a portion of the card

running path O inner than the card feeding roller 41 and at intervals longer than the length of the card. The card sensor 72 is disposed so as to be adjacent to the side of the card feeding roller 42. These card sensors are photosensors each consisting of a light emitting device and a light receiving device. Alternatively, the card sensors may be realized by using sensors of other types such as a switch.

Fig. 2 is a block diagram of the circuit of the card reader. A central processing unit (CPU) 9 consists of a microcomputer which controls the whole of the card reader. The magnetic head 2, the card sensors 71 to 73, an encoder 45 which detects the rotation of the card feed motor 40, a driver 46 which drives the card feed motor 40, the solenoid 31 which drives the shutter 3, and the information destruction magnetic head 8 are connected to the CPU 9. A reset button 91 is connected to a reset terminal.

In place of the card detection magnetic head 2, a mechanical or optical switch may be used for detecting the card insertion.

Next, the operation of the card reader will be described.

The shutter 3 is normally closed (to shut the card running path O). When a normal magnetic card C (a credit card or a prepaid card) is inserted through the card insertion slot, the magnetic head 2 detects the magnetic stripe (not shown) of the card and the solencid 31 is driven. This drive causes the

shutter 3 to be opened so that the magnetic card C is inserted into the inner portion (the insertion is manually conducted). Simultaneously, the card feed motor 40 is driven so that the card feeding rollers 41 to 43 are rotated. When the front end of the magnetic card C reaches the card feeding roller 41, the magnetic card C is transported in the card running path O by the card feeding roller 41.

When the magnetic card C reaches the magnetic head 5 and further runs, magnetic information stored in the magnetic stripe is read. When the card sensor 72 does not detect the magnetic card C any longer, it is judged that the magnetic card C has passed over the magnetic head 5, and then the card feed motor 40 is caused to reversely rotate so that the magnetic card C is returned.

When information stored in the magnetic card C is to be updated, the magnetic card C is reciprocally moved two or three times with respect to the magnetic head 5 so as to be subjected to the processes of reading and writing information. This operation is well known, and therefore its detail description is omitted.

Next, the operation of detecting the stoppage of the magnetic card (the operation is controlled by the CPU 9) will be described with reference to a flowchart of Fig. 3.

The card reader is set to be in the operation enabled state, and the CPU 9 is set.

When the normal magnetic card C is inserted through the

card insertion slot 1 under this condition, the magnetic head 2 detects the card, the solenoid 31 is driven so that the shutter 3 is raised in Fig. 1, and the card feed motor is driven. Therefore, the card running path O is opened and the magnetic card C can be inserted into the reader. When the front end of the card reaches the card feeding roller 41, the card is caused to run by the transporting force exerted by the rollers 41 and 61.

When the magnetic card C reaches the sensor 71, a timer incorporated in the CPU 9 starts the time count operation. When the magnetic card C fails to reach the sensor 72 before an elapse of, for example, 3 sec., it is judged that the card is stopped, and an emergency stop operation is conducted on the card reader. The time period is set to be 3 sec. because of the following reason. When the card reader operates normally, the time period required for a card to reach the sensor is about 1/10 times the preset emergency stop time period (i.e., 0.2 to 0.3 sec.). In consideration of variations in operation, the time period is set so as to provide a margin.

If the magnetic card C runs normally, the sensor 72 detects the magnetic card C at an elapse of a time period as short as 0.2 to 0.3 sec. after the sensor 71 detects the magnetic card C, and therefore such an emergency stop never occurs.

When the magnetic card C reaches the sensor 72, a timer incorporated in the CPU 9 starts the time count operation.

When the magnetic card C fails to completely pass over the sensor 72 before an elapse of, for example, 3 sec., it is judged that the card is stopped, and an emergency stop operation is conducted on the card reader.

If the magnetic card C runs normally, the magnetic card C completely passes over the sensor 72 within a short time period after the sensor 71 detects the magnetic card C, and the sensor 72 is then turned off. Therefore, such an emergency stop never occurs.

When the magnetic card C completely passes over the sensor 72, a timer incorporated in the CPU 9 starts the time count operation and the card feed motor 40 is caused to reversely rotate so that the magnetic card C runs in the opposite direction. When the magnetic card C fails to reach the sensor 71 before an elapse of, for example, 3 sec., it is judged that the card is stopped, and an emergency stop operation is conducted on the card reader.

If the magnetic card C runs normally, the sensor 71 detects the magnetic card C within a short time period after the magnetic card C passes over the sensor 72, and therefore, such an emergency stop never occurs. Thereafter, this condition is kept until the card is discharged.

The card sensor 73 is located at a position which is inner than the card sensor 72, in order that, in the case where the magnetic card C is stopped at a position inner than the card sensor 72, the stoppage position is determined.

When magnetically stored information is to be updated as described above, the card feed motor 40 is caused to forward rotate in response to the card detection of the sensor 71, so that the above-mentioned operation is repeatedly conducted, whereby the card is reciprocally moved over the magnetic head 5 several times required for the update of magnetically stored information. Thereafter, the operation is finished.

Next, the operation of destroying stored information of a magnetic card (controlled by the CPU 9) will be described with reference to a flowchart of Fig. 4.

Under the initial condition shown in Fig. 3, the card reader is set to be in the operation enabled state, and the CPU 9 is set.

As described above, in this condition, the timers incorporated in the CPU 9 are turned ON/OFF in response to signals from the respective sensors 71 and 72 which detect the passage of the card C, and the CPU 9 monitors the magnetic card C to see whether the card is subjected to the emergency stop operation shown in Fig. 3 or not, on the basis of elapses of the preset time periods of the timers.

If the emergency stop operation is detected, the movement of the magnetic card C is monitored on the basis of the presence or absence of an output of the encoder 45. Specifically, the encoder 45 detects the rotation of the card feed motor 40 driven by the card feeding rollers 41 to 43 which are rotated in accordance with the movement of the card C, and

produces an output. On the basis of the presence or absence of the output of the encoder 45, therefore, it is possible to monitor the movement of the magnetic card C. When the output of the encoder 45 is supplied to the CPU 9 after an emergency stop, the information destruction magnetic head 8 is driven so as to generate a strong magnetic field.

This condition is kept until all the card sensors 71 to 73 do not detect the magnetic card C. When the magnetic card C is fraudulently pulled out, therefore, the magnetic stripe of the magnetic card C passes through the strong magnetic field of the information destruction magnetic head 8, and therefore stored information is destroyed by the strong magnetic field. It is sufficient for the destruction to be conducted on only a part of the stored information. The part of stored information can surely be destroyed by the operation of pulling out the card.

When the emergency stop is to be corrected, the operator presses the reset button so that the CPU is reset. This causes the information destruction magnetic head 8 not to be driven, and hence information stored in the magnetic card C is prevented from being destroyed.

The embodiment described above is a preferred example of executing the invention. However, the invention is not restricted to the embodiment, and may be executed in variously modified manner without departing from its spirit.

For example, the stored information destruction device

may be realized by conducting a deforming process such as punching, scratching, or projection (embossment or the like) on the stripe portion of the magnetic card C by using a punch which is intermittently driven, thereby disabling the card from being reused. When the magnetic stripe is once deformed or at least uneven portion is formed in the stripe, information cannot be read, and hence it is substantially impossible to reuse the magnetic card.

The intermittent driving of the punch is conducted because the timing when the magnetic card C passes below the punch cannot be specified.

When the magnetic card C is heated to a temperature higher than the Curie point, magnetic information of the stripe is destroyed. Consequently, heating device such as a heater which can heat the card to a temperature of about 200 °C may be used as the stored information destruction device.

Alternatively, the information destruction device may be realized by advancing a file or the like into the card running path so as to oppose the stripe, and then scratching the stripe.

As described above, according to the invention, a magnetic card reader of the card running type is constructed so that, when a magnetic card which stops in the reader is pulled out, the stored information destruction device destroys stored information. Even when device for stopping a card is intentionally disposed in the reader and a magnetic card of

another person which stops in the reader is stolen from the reader, therefore, it is possible to prevent the stealing from producing a victim. When a magnetic head or a heater is used as the stored information destruction device, particularly, it is possible to attain an effect that the stealer cannot recognize the fact that stored information is destroyed. The invention may be applied to a magnetic card reader which is already in operation.

**CLAIMS**:-

1. A method of preventing a card with stored information data from being fraudulently used in a card reader of the card running type, said method comprising the step of destroying at least a part of the information data stored in the card by an information destruction device when the card is fraudulently pulled out from the card reader.

2. The method of claim 1 wherein said information destruction device is activated in response to a movement of the card detected by a movement detecting device after detecting an abnormal stoppage of the card by a stoppage detecting device.

3. The method of claim 2 wherein said stoppage detecting device includes card sensors arranged in a card running direction and at intervals which are shorter than a length of the card.

4. The method of claim 3 wherein the card fails to completely pass over one of said card sensors in a predetermined time, it is judged to be subjected to an abnormal stoppage, thereby the card reader being stopped.

5. The method of claim 4 wherein said movement detecting device includes card sensors arranged in a card running direction and at intervals which are shorter than a length of the card.

6. The method of claim 3 wherein when the card does not reach one of said card sensors in a predetermined time after being detected by the adjacent one, it is judged to be subjected to an abnormal stoppage, thereby the card reader being stopped.

7. The method of claim 6 wherein said movement detecting device includes card sensors arranged in a card running direction and at intervals which are shorter than a length of the card.

8. The method of claim 4 wherein said movement detecting device includes an encoder for detecting a rotation of a motor for feeding the card.

9. The method of claim 6 wherein said movement detecting device includes an encoder for detecting a rotation of a motor for feeding the card.

10. The method of claim 1 wherein said information destruction device includes an erasing member electromagnetically generating a strong magnetic field.

11. The method of claim 10 wherein said erasing member is on a side of a card insertion slot in a card running path of the card reader.

12. The method of claim 1 wherein said information destruction device includes a heater member generating a heat.

13. The method of claim 12 wherein said heater member is on a side of a card insertion slot in a card running path of the card reader.

14. The method of claim 1 wherein said information destruction device includes a deforming member deforming the card.

15. The method of claim 14 wherein said deforming member is on a side of a card insertion slot in a card running path of the card reader.

16. A card reader device of the card running type for preventing a card with stored information data from being fraudulently used, said card reader comprising:

a stoppage detecting device for detecting an abnormal stoppage of the card,

a movement detecting device for detecting a movement of the card after the abnormal stoppage; and

an information destruction device for destroying at least a part of the information data, said information destruction device being activated in response to the movement of the card detected by said movement detecting device.

17. A method substantially as described herein with particular reference to Figures 3 and 4 of the accompanying drawings.

18. A device substantially as described herein with particular reference to Figures 1 and 2 of the accompanying drawings.

17

| Patents Act 1977<br>Examiner's report to the Comptroller under Section 17<br>(The Search report) | Application number<br>GB 9519627.5 |
|---|---|
| **Relevant Technical Fields**<br>(i) UK Cl (Ed.N) G4M (MAW)<br>(ii) Int Cl (Ed.6) G06K 7/00, 7/01, 7/08, 17/00 | Search Examiner<br>J DONALDSON<br>Date of completion of Search<br>26 OCTOBER 1995 |
| **Databases** (see below)<br>(i) UK Patent Office collections of GB, EP, WO and US patent specifications.<br>(ii) ONLINE: WPI | Documents considered relevant following a search in respect of Claims :-<br>1 TO 18 |

**Categories of documents**

| | | | |
|---|---|---|---|
| X: | Document indicating lack of novelty or of inventive step. | P: | Document published on or after the declared priority date but before the filing date of the present application. |
| Y: | Document indicating lack of inventive step if combined with one or more other documents of the same category. | E: | Patent document published on or after, but with priority date earlier than, the filing date of the present application. |
| A: | Document indicating technological background and/or state of the art. | &: | Member of the same patent family; corresponding document. |

| Category | Identity of document and relevant passages | | Relevant to claim(s) |
|---|---|---|---|
| X | US 4322613 | (OLDENKAMP) see column 2 line 16 - column 3 line 2 | 1. 10. 11 |

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).